APPENDIX

Life-Cycle Management-

Internal Control

Techniques

This is the first attempt to integrate control techniques with the life-cycle phases. The results indicate there is room for refinement and identification of additional control techniques, especially in the early phases.

The items shown in bold (and solid bullet), below, identify those tasks and products that are required for each LCM Phase of an AIS project. AIS internal control techniques to be considered when developing those tasks or products are included (not in bold) under the appropriate LCM bullets. The AIS internal control techniques are from Chapter 6.

A. Need Justification (Phase 0)

1. • Identification of Mission Deficiency.

o Functional or Operational.

a. AIS Planning

(1) An AIS management process that considers inputs from the various involved organizations, including major user departments and program areas, should be applied to justify the need for new automated equipment.

(2) The planning process should establish and document mission requirements, strategy, and overall system goals and objectives.

2. • Conduct Analyses.

o Security or other vulnerability analyses.

o Characterizing the current and projected environment to include wartime role, if any.

o Estimated Time And Cost for Corrective Action (level of effort).

o Standardization, Integration, and Interface Requirements.

a. AIS Planning

(1) An AIS management process that considers input: from the various involved organizations, including major user departments and program areas, should be applied to ensure that new equipment is acquired in the most economical and expedition manner.

(2) AIS planning should be related to budgeting for financial, personnel, and system resources.

(3) The AIS planning process should take into account relevant computer security requirements affecting the scope of ADP activity.

b. Policies, Standards, and Procedures

(1) Policy and procedures should be established to comply with systems security, privacy, and freedom of information requirements.

c. Internal Audit

(1) Internal Audit should actively participate in reviewing the development of new systems or applications and th significant modification of existing systems.

d. Distributed Processing and Network Operations Controls

(1) The operating provisions in the implementation plan should be consistent with the laws and regulations governing transmission of data within the country and/or internationally.

•Information Reporting Requirements Approved in Accordance with DoD Directive 7750.5 (reference (p)).

a. AIS Planning

(1) The AIS planning process should establish and document individual responsibility for specific actions to be undertaken.

b. System Reporting Documentation Controls

(1) A functional requirements document should be prepared to provide the basic understanding between users and designers of the system.

(2) A data requirements document should be prepare to provide a data description and technical information about data collection requirements.

4. •Preparation of Mission Need Statement (MNS) .

a. AIS Planning

(1) The planning process should establish and document mission requirements, strategy, and overall system goals and objectives. -

b. Systems Development Methodology Controls

(1) The system development process should include user need definition.

5. " Submission of MNS to LCM review and milestone approval authority.

a. Policies, Standards, and Procedures

(1) Rigorous AIS budgeting procedures should be implemented to ensure that all significantly ADP-related initiatives, expenditures, and reprogramming are clearly highlighted, whether or not they fall within budget decision units or are spread over multiple decision units.

b. Systems Development Methodology Controls

(1) Formal requests for new or revised systems should be prepared by users submitted with proper authorization and used to develop the conceptual system design.

c. System Reporting Documentation Controls

(1) A project request document should be prepared to provide the means for a user to request the development , procurement, or modification of software or other AI S-related services.

B. Concepts Development (Phase 1)

1. •Mission Need Reaffirmed.

2. • Project Manager Appointed and Chartered.

a. AIS Planning

(1) The AIS planning process should establish and document individual responsibility for specific actions to be undertaken.

b. System Development Methodology Controls

(1) A formal management controlled approach for system development should exist.

(2) The project manager should be authorized to make decisions on personnel resources, scheduling, and most technical project matters.

(3) A management project steering committee should be formed to oversee and review progress throughout the life cycle.

3. • Functional Objectives Prioritized.

a. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

(2) Rigorous project control and performance measurement techniques (e.g., PERT, CPM) and progress reportin should be required based upon actual cost and work-year expenditures, deliverables provided, and milestones achieved (rather than upon subjective percent of completion estimates).

b. Distributed Processing and Network Operations Controls

(1) A central control function should be established to coordinate control reviews of network assets an resources at all network locations.

(2) Network output requirements, operating schedules, processing procedures and facility coordination policies should be fully established.

(3) policy agreements should exist for communications transmissions, including provisions to effectively interface software applications and data bases amo coordinated network facilities.

c. Systems Development Methodology Controls

(1) The system development process should include user need definition.

(2) Procedures should exist to ensure that no data is lost or erroneously changed during conversion to the newly designed system.

(3) Users should actively participate in system development.

d. Data Input Controls

(1) Data validation and editing should be performe as early as possible in the data flow to insure that the

application rejects any incorrect transaction before its entry into the system.

4. • Develop Functional Descriptions.

a. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

b. Distributed Processing and Network Operations Controls

(1) Policy agreements should exist for communications transmissions, including provisions to effectively interface software applications and data bases among coordinated network facilities.

c. Systems Development Methodology Controls

(1) Users should actively participate in system development.

d. System Reporting Documentation Controls

(1) A data requirements document should be prepared to provide a data description and technical information about data collection requirements.

5. • Demonstrate Feasible Alternatives.

a. AIS Planning

(1) AIS planning should be related to comparing and selecting among system alternatives based upon quantified life-cycle cost, benefit, "and risk projections.

b. Systems Development Methodology Controls

(1) The conceptual system design should be used to determine the technical and operational feasibility of the system.

c. System Reporting Documentation Controls

(1) A cost-benefit analysis document should be prepared to give managers, users, designers, and auditors adequate information to evaluate alternative approaches for significant system additions or modifications.

6. • Update Cost and Time Estimates.

a. AIS Planning

(1) An AIS management process that considers inputs from the various involved organizations, including major user departments and program areas, should be applied to ensure that new equipment is acquired in the most economical and expeditious manner.

(2) AIS planning should be related to budgeting for financial, personnel, and system resources.

b. Systems Development Methodology Controls

(1) Specific tasks and timeframes for completing the tasks should be established for each member of the development project.

c. System Reporting Documental ion Controls

(1) A cost and/or benefit analysis document should be prepared to give managers, users, designers, and auditors adequate information to evaluate alternative approaches for significant system additions or modifications.

7. • Preliminary Planning (Training, Log) .

a. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

b. Policies, Standards , and Procedures

(1) All appropriate organizational components of the site involved with ADP systems should be defined and clearly assigned their respective areas of functional responsibility.

(2) Procedures describing the manner and responsibility for performance between users and ADP should be established, coordinated, and communicated to all affected organizations.

c. Organizational Controls

(1) The ADP function should be placed sufficiently high in the organization to ensure its independence from other site operations.

(2) Major organizational units within ADP should be described and their responsibilities delineated and documented.

(3) Training programs should exist to maintain and build skills, knowledge, and ability in systems technology as well as internal control and ADP security requirements .

d. Workload Scheduling Controls

(1) Formal input and/or output control procedures should be established and documented.

(2) The control group should establish and document formal scheduling procedures, schedule production runs and other workloads, and reschedule aborted or erroneous processing.

e. Malfunction Reporting and Preventive Maintenance Controls

(1) Formal malfunction reporting procedures should be established and documented for the data processing installation.

f. User Billing and Charge-back Controls

(1) Procedures for user billing and charge should be documented.

g. Distributed Processing and Network Operations Controls

(1) The distributed processing requirements definitions should be responsive to management objectives in terms of the hardware configuration, data base configuration and hardware, and communications network interface.

(2) The operating provisions in the implementation plan should be consistent with the laws and regulations governing transmission of data within the country and/or internationally.

(3) Network data policies should require that data set ownership be clearly established.

(4) Policy agreements should exist for communications transmissions including provisions to effectively interface software applications and data bases among coordinated network facilities.

h. Data Origination Controls

i. Data Input Controls

j. Data Processing Controls

k. Data Output Controls

1. Microcomputer Controls

8. " Develop Acquisition Strategy.

9. •Standardization and Interoperability.

a. Distributed Processing and Network Operations Controls

(1) The operating provisions in the. implementation" plan should be consistent with the laws and regulations governing transmission of data within the country and/or internationally.

(2) Appropriate techniques and policies should be instituted for standardizing data definitions of shared data, maintaining common data dictionaries, and reconci ling deviat ion in data definition at remote facilities.

10. •Areas of Risk and Uncertainty Identified.

a. Internal Audit

(1) The responsibility of the internal audit function in relation to ADP should be clearly documented.

b. Administrative Controls

(1) Responsibility for conducting risk analyses should be formally assigned.

(2) Risk analysis studies should measure vulnerability related to the potential for the following:

(a) Fraud or theft,

(b) Inadvertent error or improper disclosure of information,

(c) Financial loss,

(d) Harm to individuals or infringement on privacy rights,

(e) Loss of proprietary data and harm to organizational activities.

(3) A Specific timetable for conducting risk analysis studies should be established, with the time between studies'being commensurate with the sensitivity of the information processed.

(4) Procedures should require that a risk analysis be performed before the approval of design specifications for computer installations or whenever significant changes are made

to the physical facility, hardware, or operating system software.

11. • Develop AIS Transition Strategy.

12. • Establish Configuration Management Discipline.

a. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

13. • Electronic Countermeasure Requirements.

14. • Plan for Preparation of T&E Plan.

a. Policies, Standards, and Procedures

(1) Rigorous project control and performance measurement techniques (e.g., PERT, CPM) and progress reporting should be required based upon actual cost and work-year expenditures, deliverables provided, and milestones achieved (rather than upon subjective percent of completion estimates).

15. • Communications Requirements.

16. • Privacy and Security Requirements.

a. AIS Planning

(1) The AIS planning process should take into account relevant computer security requirements affecting the scope of ADP activity.

17. • Contractor vs. In-House Analysis.

a. AIS Planning

(1) An AIS management process that considers input from the various involved organizations, including major user departments and program areas, should be applied to assure that new equipment is acquired in the most economical and expeditious manner.

(2) AIS planning should be related to comparing and selecting among system alternatives based upon quantified life cycle cost, benefit, and risk projections.

18. • Preparation of System Decision Paper (SDP-1).

19. " Submit SDP to LCM review and milestone approval authority.

a. AIS Planning

(1) AIS planning should be related to comparing and selecting among system alternatives based upon quantified life-cycle cost, benefit, and risk projections. A full cost benefits analysis is not expected until Milestone 11.

(2) The planning process should measure and compare actual accomplishments with expected performance throughout the system life cycle.

b. Systems Development Methodology Controls

(1) A formal management cent rolled approach for system development should exist.

(2) The system development process should include conceptual system design.

(3) Formal requests for new or revised systems should be prepared by users submitted with proper authorization and used to develop the conceptual system design.

(4) The conceptual system design should be used to determine the technical and operational feasibility of the system.

C. Design (Phase 2)

1. • Mission Need Reaffirmed.

a. AIS Planning

(1) Regular internal audit review and reporting should be conducted regarding completed and proposed planning decisions in relation to mission requirements.

2. • Functional System Design Revalidated.

o Baseline Updated.

a. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

b. Systems Development Methodology Controls

(1) The conceptual system design should be used to determine the technical and operational feasibility of the system.

3. “ Develop AIS Specifications for hardware, software and databases.

a. Data Origination Controls

(1) Special forms should be used to guide the initial recording of data in a uniform format.

(2) Source documents should be designed in such a manner as to minimize errors and omissions and to ensure data uniformity.

(3) Source documents should be pre-numbered, if appropriate.

(4) For each type of transaction, the source document should provide a unique identifying code.

(5) Each transaction should have a cross-reference number that can be used to trace data to and from the source document.

b. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

c. Technical Controls

(1) Separate security software should be used to provide control over the site' s computer resource.

(2) The security software should control access to terminals, remote job entry station, individual automated data files, application programs, and other system software;

(3) Security software functions should be adequately supported by proper manual procedures.

(4) The vendor or developer of the security software should provide a completely documented description of its design and operation.

(5) The control functions performed by security software should not be able to be overridden or bypassed.

(6) The security software should provide an audit trail of all authorized uses and unauthorized attempted accesse of computer resources under control.

(7) The security software should control access to data in a different manner than access to other computer resources.

(8) The security software should be transparent to all application programs and to all other system software.

(9) In an on-line environment, there should be access security control based on the classification of file data and devices.

(lo) Sensitive files, such as security classifications or Privacy Act restrictions, should be properly identified as such, and appropriately secured.

d. Operating Systems Controls

(1) The operating system should prohibit one application program from accessing memory or data of another application program that is processing simultaneously.

(2) The use of privileged instruction of the operating system should be strictly controlled.

(3) The operating system should prohibit an application program from accessing operating system instructions, password tables and other security algorithms.

(4) The operating system should prohibit operators from entering application data or changing users' memory values at the computer console.

(5) The operating system should control all input and or output functions of data files.

(6) Operating system instructions, password tables, and other authorization algorithms should be protected from unauthorized access when the computer system fails.

(7) Provisions should be made to prohibit application programs from overriding or bypassing errors that are detected during processing.

(8) All application programs or other system software should be run only when the operating system is operational.

(9) An audit trail of all operating system actions should be maintained either on the automatic console log or as part of the computer system's job accounting data.

(10) The computer system's internal clock should be adequately protected from unauthorized access.

(11) The operating system should adequately and accurately schedule all jobs run on the computer system.

e. System Utilities Controls

(1) Controls that detect processing errors in system utilities should not be able to be overridden or bypassed.

(2) System utilities should not be able to be used to override or bypass controls within other system so ftware or application programs.

f. Program Library Systems Controls

(1) A program library system should be used to control application programs.

(2) The program library system should restrict access to application programs , control movement of programs from test to production modes, control movement of programs from source code to object code, and control changes to application programs.

(3) Control functions performed by the program library system should be protected so they cannot be bypassed.

(4) The program library system should provide an audit trail of all changes made to application programs.

(5) The program library system should prevent the existence of more than one version of a source code and object code program.

g. File Maintenance Systems Controls

(1) A file maintenance system should be used to control all disk and tape data set.

(2) The file maintenance system should control the establishment, use, and retention of automated data files.

(3) Functions of the data communications system should be protected so that they cannot be overridden or bypassed.

(4) A built-in hardware identification code should be checked by the data communications system to ensure that no unauthorized terminals are being used.

(5) The data communications system should use a table of authorized terminal addresses to allow polling with the communications network.

(6) Control functions performed by the file maintenance system should be protected so that they cannot be overriden or bypassed.

(7) The file maintenance system should include redundancy controls such as prohibiting more than one data file from having the same volume serial number.

(8) User authorization codes or passwords should be required by the data communications system to access the computer system and application programs, other system software ***and to enter transactions.***

(9) Different authorization codes should "be required to enter different types of transact ions.

(10) The authorization code should identify the individual using the terminal and should be periodically changed.

(11) A nonprinting and/or nondisplaying facility should be used when keying in and acknowledging user authorization codes.

(12) A terminal identification check should be performed by the data communications system so that various transaction types can be limited to authorized data entry stations.

(13) The security matrix or table used to control access to the application system should be properly protected to prevent unauthorized access.

h. Data Communications Systems Controls

(1) A data communications system should serve as the interface between terminals and the central data processing system.

(2) Functions of the data communications system should be protected so that they cannot be overridden or bypassed.

(3) The data communications system should control access to and use of terminals, poll and receive messages from computer terminals or other computers , address and send messages back to computer terminals or other computers , edit and format input and output messages , handle error situations , reroute traffic when terminals or lines are inoperative, and perform on-line formatting on visual display terminals.

(4) A built-in hardware identification code should be checked by the data communications system to ensure that no unauthorized terminals are being used.

(5) The data communications system-should use a table of authorized terminal addresses to allow polling with the communications network.

(6) User authorization codes or passwords should be required by the data communications system to access the computer system and application programs, other system software, and to enter transactions.

(7) Different authorization codes should be required to enter different types of transactions.

(8) The authorization code should identify the individual using the terminal and should be periodically changed.

(9) A nonprinting and/or nondisplaying facility should be used when keying in and acknowledging user authorization codes.

(10) A terminal identification check should be performed by the data communications system so that various transaction types can be limited to authorized data entry stations.

(11) The security matrix or table used to control access to the application system should be properly protected to prevent unauthorized access.

(12) A message header should be used by the data communications system to identify the source of the message, including proper terminal and use authorization code, message sequence number, including total number of message segments, transportation type code, and transportation authorization code.

(13) This message header should be validated by the data communications system for proper sequence number from the identified terminal, proper transaction code and /or user authorization code for the terminal or user, and number of message segments received equal to the count indicated in the message header, proper acknowledgment from the terminal at the end of a transmission, and balancing of debit and/or credit totals derived from adding all message segments and comparing them with corresponding totals in the message header.

(14) The data communications system should include an end-of-transmission trailer that includes message and segment, value totals, including debits and credits, if appropriate, and an ending symbol.

(15) The data communications systems should reconcile counts and totals with header counts and totals.

(16) The data communications system should send acknowledgments to the terminal indicating receipt of messages and periodically test line and terminal operating status with standardized test messages and responses.

(17) The data communications system should use buffering to queue messages when a device, such as a terminal, is busy.

(18) The data communications system should maintain a transaction log of sequentially numbered and/or time-of-day-noted transactions.

(19) The transaction log should record the originating terminal, user authorization code, message identification, transaction type code, time of day that the transaction was logged, and transaction data.

(20) The transaction log should provide part of the audit trail, account for all error messages, and record, with control totals, all retrievals made by a particular terminal.

(21) All messages awaiting transmissions should be logged by the data communications system before being put into the transmission queue and then purged after successful transmission.

i. System Software Change Controls

(1) Formal documented *system* software change procedures should be established.

(2) Procedures should be established so that the accepted emergency modifications will be incorporated into the next operational version of the system software.

(3) Procedures should be established to ensure that emergency system software modifications are immediately subjected to a system acceptance test.

j. Data Base Management Systems Controls

(1) Where appropriate, responsibility for administering the data base environment should be established a a high enough level to ensure independence.

(2) The vendor or developer of the data base management system should provide a complete documented description of its design and operation.

(3) The data base management system should provide security over data base accesses, control the addition, modification, and deletion of data, and provide a complete documented description of its design and operation.

(4) Integrity of data maintained within the data base should be ensured through utility programs that check the physical linkage of data within the database, control records

that maintain interim balances of transactions and apply application programming standards that include procedures for maintaining integrity.

(5) Data base management system functions should be adequately supported by proper manual procedures.

(6) Functions of the data base management system should be protected so that they cannot be overridden or bypassed.

(7) The use of restricted instructions should be logged and checked periodically.

(8) The data base management system should use authorization codes or passwords to control access to data items.

(9) The data base management system should record unsuccessful attempts to access the data base.

(10) The data base management system should record which application programs have accessed each data item within the data base.

(11) The data base management system should prevent simultaneous updates to a record.

(12) The data base management system should prevent shared data from being deleted without consent of all users of the data.

(13) A log should indicate whether an application program has read, updated, created, or deleted a data item.

(14) All errors discovered by the data base management system should be logged for follow-up.

(15) Failures in the data base management system should be documented for supervisory review.

(16) A data dictionary should be developed and maintained, documenting the attributes of each data item and the security over each data item.

k. Central Processing Unit Controls

(1) Built-in parity bits should be used by the CPU to ensure that all data elements transmitted through the internal circuitry are correctly transmitted.

(2) Redundant character checking should be used by the CPU to ensure the correctness of data processing.

(3) The CPU should use validity checks to ensure that only valid operation codes are used.

(4) The CPU should perform validity checks on the numbers used to access memory to ensure that only valid numbers are used.

(5) The CPU should have automatic interlock controls to prevent the equipment from performing certain operations at the wrong time.

(6) Log should be maintained to record CPU meter readings at the start and end of each shift, and variances should be explained.

1. Peripherals Controls

(1) Parity checks of both individual and blocks of data should be made to ensure that all data elements are transmitted accurately.

(2) Validity check controls should be used to chec the results of an operation with all possible valid solutions.

(3) Echo checks should be used to ensure that a transmitted command is actually performed or the data sent is correct.

(4) A read-after-write check should be used to ensure that the record just written was correctly recorded.

(5) Equipment diagnostic tests should exist for th computer to check if the equipment is functioning properly.

(6) With direct access storage devices, address comparisons should be made to verify the address to which data is to be written with the address called for by the instruction

(7) Print synchronization controls should be used to check the timing of the printer to determine that print hammers of impact printers are activated at the moment when appropriate characters are in the correct position.

4. • Communications Requirements.

a. Distributed Processing and Network Operations Controls

(1) Hardware controls should include memory protection, alternate communication routing, communication protocols, and timely failure recovery mechanisms;

(2) Software controls over reentrant operating systems and current data base accesses and update should exist

(3) Commonly shared and distributed data should be designed to readily permit integration and summarization at an organization-wide level to meet current or anticipated objectives.

(4) Adequate disaster and recovery procedures should be developed for each network processing facility. Thes e procedures should be current and periodically tested.

(5) · Network data standards should require and define data set change control procedures.

(6) Standards and policies for general network control should be clearly established and followed.

(7) Network standards and policies should be sufficiently broad-based, not to encumber local autonomy or operating objectives.

(8) As the general network capability is distributed, controls should be distributed to users.

(9) A network policy should require the ongoing identification of data set needing inter-system compatibility.

(10) A network should exist requiring audit trails and backup of all network communications activity for both network messages and application processed data.

(11) A network implementation, conversion and acceptance plan should be developed jointly by systems and network user organizations and include user-prescribed test procedures and acceptance criteria.

(12) User and system responsibilities should be fully defined for coordinating and reconciling differences between distributed and/or replicated data bases prior to network implementation.

(13) Reconciliations should be able to be satisfactory performed under normal conditions, following network failures, and between varying application problems.

(14) Each network message and/or transmitted data unit should contain codes that identify the sender and intended receiver(s) .

(15) All changes made to network operating systems software at remote processing facilities should be controlled by the central and/or main network processing facilities.

(16) A network data review mechanism should be established to administer compatibility between system and data as the network grows.

b. Systems Development Methodology Controls

(1) The system -development process should include detailed system analysis and design.

(2) Planning for the new facility to include reliable power, (UPS) , communications lines, air conditioning, raised floors, (if applicable) , fire protection equipment.

(3) Additional hardware and system software requirements should be consistent with ADP plans and be included in the cost and/or benefit analysis, and be used to prepare the computer programs.

(4) Users should actively participate in system development.

(5) The detailed system design should be consisten with the conceptual design, be based on the feasibility study and on the cost-benefit analysis, and be used to prepare the computer programs.

c. System Reporting Documentation Controls

(1) Detailed system and/or subsystem specification should be developed.

(2) Detailed program specifications should be developed for all programs of the system.

(3) Detailed specifications should be developed fo data bases used by the system.

d. Data Origination Controls

(1) Duties should be separated to ensure, unless authorized, that no one individual performs more than one of th following: originating data, entering data, processing data, 01 distributing output .

(2) Access to source documents , blank input forms , and copies of source documents should be restricted to authorized personnel only.

(3) Authorizing signatures should be used for all paper transactions, when required.

(4) Duties should be separated within the user organization to ensure, unless authorized, that one individual does not prepare more than one type of transaction.

(5) Duties should be separated within the user organization to ensure, unless authorized, that no one individual performs more than one of the following: originating the source document, authorizing the source document, or controlling the source document.

(6) The user organization should have a control group responsible for collecting and completing source documents.

(7) This control group should verify that source documents are complete and accurate. Furthermore, all documents should be accounted for, be transmitted in a timely manner, and have been appropriately authorized.

(8) A separate user group should perform the input function when the user organization is responsible for its own data entry.

(9) The control group should identify errors to facilitate the timely correction of erroneous information.

(10) Error logs should be used to ensure timely follow-up and correction of unresolved errors.

(11) Originators of source documents should be notified by the control group of all errors.

e. Data Input Controls

(1) Password controls should be used to prevent unauthorized use of terminals.

(2) When keying passwords and authorization codes, nonprinting and nondisplaying facilities should be used.

(3) An immediate report should be produced of unauthorized attempts to access the system via terminals.

(4) Terminal hardware features should include the following:

(a) Built-in terminal identifications that automatically validate proper terminal authorization.

(b) Terminal logs that record all transactions processed.

(c) Record counts that are automatically accumulated for logging purposes.

(5) Parity checking should be used to check each character and each message.

(6) Error messages should promptly be displayed with clearly understood corrective actions for each type of error.

(7) All data that does not meet edit requirements should be rejected from further processing by the application, produce an error message, and be written on an automated suspense file.

(8) The suspense file should include the date and time a transaction was entered along with the identity of the user who originated the transaction.

(9) Suspense file processing should create record counts and predetermined control totals.

(10) Valid correction transaction should purge the automated suspense file of corresponding rejected transactions.

(11) The suspense file should be used to control follow-up, correction and reentry of rejected transactions.

(12) Debit and/or credit entries, rather than delete or erase commands, should be used to correct errors on the suspense file.

(13) Record counts and predetermined control totals should be appropriately adjusted by correcting transactions.

(14) "Intelligent" terminals should be used to allow front-end validation, editing and control.

(15) Data validation and editing should be performed as early as possible in the data flow to ensure that the application rejects any incorrect transaction before its entry into the system.

(16) Preprogrammed keying formats should be used to make sure that data is recorded in the proper field, format .

(17) Computer-aided instruction, such as prompting, should be used with on-line dialog to reduce the number of operator errors.

(18) Batch control totals, record counts, and predetermined control totals submitted by the data processing control group should be used by the computer-based system to validate the completeness of data input into the application.

(19) Data validation and editing should be performed for all input data fields.

(20) Input document should be retained in a manner that enables tracing them to related originating documents and output records.

(21) All converted documents and input documents returned to the data processing control group should be logged in and accounted for.

(22) Procedures for processing corrected transactions should be the same as those for processing origina transactions, except for the supervisory review and approval.

(23) The ultimate responsibility for the completeness and accuracy of all application processing should remain with the user.

(24) The terminal user should correct errors caused by data conversion or entry.

(25) The user originating the transaction should correct errors not caused by data conversion or entry.

(26) All documents entered into the application should be signed or marked in some way to prevent accidental duplication or. reuse of the data.

(27) The data processing organization should have a control group responsible for data conversion and entry of all source documents received from users.

(28) With proper password protection, personnel should not be able to bypass validation and editing problems.

f. Data Processing Controls

(1) The data processing organization should have a control group responsible for controlling all data processing operations.

(2) Application programs should be prevented from accepting data from computer ‘con-soles.

(3) The system should have a history log that is printed on both a line printer and the console.

(4) Each input transaction should have a unique identifying transaction ‘code that directs it to the proper application program for processing.

(5) Standardized default options should be built into the program logic.

(6) Computer-generated control totals (run-to-run totals) should automatically be reconciled to check for completeness of processing.

(7) Controls should be in place to prevent operator from circumventing file checking routines.

(8) Controls should ensure that output counts equal input counts.

(9) All programs that include a table of values should have an associated control mechanism to ensure accuracy of the table value.

(10) There should be an audit trail in the application to assist in reconstructing data files.

(11) Messages and data should be able to be traced back to the user or" to the point of origin.

(12) The application should prevent concurrent file updates".

(13) Transactions should be date and time stamped for logging purposes.

(14) There should be controls to verify that proper data is used when computerized data is entered into the compute] application.

(15) When computerized files are entered into the computer application, there should be controls to verify that the proper version of the file is used.

(16) Application programs should include routines for checking internal file header labels before processing.

(17) Internal trailer labels should contain control totals to provide a check that all records are on the file.

(18) File completion checks should be performed to ensure that application files have been completely processed, including both transaction and master files.

(19) Record and predetermined control totals generated by the application should be used by the data processing control group to validate the completeness of data processed by the system.

(20) A direct update to files should cause creation of a record added to a backup file and recording of the transaction on the transaction history file.

(21) A "before and after picture" of the master fil being updated should be maintained.

(22) Relationship editing should be performed between the input transaction and master files to check for appropriateness and correct-ions prior to updating.

(23) The data processing control group should balance batch counts, record counts, and predetermined control totals of data submitted for processing; ensure that input and/or work and/or output files used in computer processing ar correct and maintained in logs; and ensure that restarts are properly performed.

g. Malfunction Reporting and Preventive Maintenance Controls

(1) The computer system should automatically produce a log of all-system operations.

(2) Disposition notes should be entered on the console log showing corrective actions taken when unscheduled program halts occur.

(3) Job reruns should be recorded along with their reason on the console log.

(4) The console log, should include the date, job name and number, program name and number, start and/or stop times, files used, record counts, and scheduled and unscheduled halts.

(5) All computer time should be accounted for.

(6) Sensitive data should be removed from on-line storage devices before equipment is turned over to maintenance personnel.

(7) System reliability reports should include Mear Time Between Failures (MTBF) and Mean Time To Recovery (MTTR) statistics.

h. Data Output Controls

(1) The data processing organization should have a control group that is responsible for reviewing all outputs produced by the application.

(2) This group should reconcile each output batch total, record count and predetermined control total with input batch totals, and record counts and predetermined control tota before releasing any reports in order to ensure that no data w added or lost during processing.

(3) A transaction log kept by the application should be compared regularly with a transmission log kept at each output device to ensure that all transactions have been properly processed to the final output steps.

(4) The user should have a control group that is responsible for reviewing all output received from the data processing organization.

(5) System output logs should be kept to provide an audit trail for the outputs and to summarize the number of reports generated, the number of copies of each report, the recipients of each report and the report security status.

(6) Transactions should be able to be traced forward to the final outputs and backward to the original source documents.

(7) The cover sheet of every report should clearly identify the recipients' names and locations.

i. Data Communications Controls

(1) Controls over data communication devices should be established and followed to ensure accuracy and privacy of transmitted data. The following control techniques should exist within data communication devices:

(a) A unique hard-wired identification code, requiring no human intervention for its use, should be incorporated into each terminal device;

(b) The identification code should be checked and validated by the computer to ensure that no unauthorized terminals are being used;

(c) Conditioned lines should be used to reduce data transmission errors and to maintain integrity of data transmitted;

(d) Scrambling or encryption techniques should be used in transmitting classified data;

(e) An automatic store-and-forward capability should be used to maintain control over messages queued for an inoperative or for a busy communications device;

(f) Parity checks should be used to detect errors in the transmission of data;

(g) Validity checks should be used to compare characters so that erroneous data can be detected;

(h) Forward error correcting techniques should be used for the detection and reporting of data communications errors using sophisticated redundancy codes;

(i) Techniques should be available for detecting erroneous retransmissions of data;

(j) Modems should be equipped with loop-back switches for fault isolation.

(k) A message intercept function should be used to receive messages directed to inoperable or unauthorized terminals.

5. Update Plans for Training, Log, Support, T&E, Development and Acquisition.

a. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

b. Workload Scheduling Controls

(1) A formal control group should be established within the data center to monitor both remote decentralized as well as centralized job entry.

(2) The control group should be responsible for recording and controlling the production data processed by the data processing organization.

(3) All totals should be balanced during and after applications processing, and all processing errors should be controlled by the control group.

(4) An authorization document or a transmittal sheet should be required to accompany all input transactions.

(5) All output reports should be visually scanned by the control group for general accuracy and completeness and be distributed according to a formal schedule.

(6) A priority scheme of classes or priorities should be used for scheduling work.

(7) Source documents should be maintained for reference in a logical sequence for a suitable period of time.

(8) A systematic time-related flow of jobs through each work center should be established.

c. Organizational Controls

(1] Transactions generally should originate and be authorized in an organization outside of ADP.

(2) Training programs should exist to maintain and build skills, knowledge and ability in systems technology, as well as internal control and-ADP security requirements.

d. Internal Audit

(1) During system planning and development, internal audit should ensure that the system carries out prescribed management policies.

(2) Internal audit should review general controls in data processing systems to determine that controls have been designed according to management direction and legal requirements and that these controls are operating effectively to provide reliability of, and security over, the data being processed.

e. Distributed Processing and Network Operations Controls

(1) Each network message and/or transmitted data unit should contain codes that identify the sender and intended receivers] .

(2) Adequate security should exist and be periodically reviewed over data controlled by network data base management systems and application and/or transaction processor and over data handled at network processing facilities and remote locations.

(3) Review procedures for identifying and handling sensitive data should exist, and security classification for al levels of data sets in the network should be developed, consistent with information classification requirements .

[4) Procedures stating the preferred method for disposing of sensitive network documents at remote locations should exist and be communicated to the appropriate personnel.

(5) All outgoing messages and/or data units should be edited for valid destination addresses.

f. Disaster Avoidance and Recovery

(1) Procedures should include steps to be. taken in the event of an actual or likely natural disaster by fire, wate damage, and intentional damage by sabotage, mob action, bomb threats .

(2) Procedures should exist and be applied for the retaining and/or copying of master files as a means of reconstructing a damaged or destroyed file.

g. Data Communications Systems Controls

(1) A data communications system should serve as the interface between terminals and the central data processing system.

(2) The data communications system should control access to and use of terminals, poll and receive messages from computer terminals or other computers, address and send messages back to computer terminals or other computers, edit and format input and output messages, handle error situations, reroute traffic when terminals or lines are inoperative, and perform on-line formatting on visual display terminals.

6. . Risk Analysis Reassessed.

7. • Economic Analysis Prepared (DoD Instruction 7041.3) (reference (q)).

a. Distributed Processing and Network Operations Controls

(1) The decision to undertake distributed processing should be documented and supported by cost and/or benefit analysis studies.

(2) A cost and/or benefit analysis of encryption and private line acquisition should be made.

b. Systems Development Methodology Controls

(1) The system development process should include cost and/or benefit analysis.

(2) A cost and/or benefit analysis should be performed to ensure that the conceptual system will produce desired results economically.

(3) Additional hardware and system software requirements should be consistent with ADP plans and be included in the cost and/or benefit analysis, and be used to prepare the computer programs.

(4) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost and/or benefit analysis, and be used to prepare the computer programs.

8. • Configuration Management Discipline for Total AIS Developed.

9. • Computer Resource Acquisition Plans Finalized.

a. AIS Planning

(1) The planing process should measure and compare actual accomplishments with expected performance throughout the system life cycle.

10. •Preparation of System Decision Paper (SDP-II).

a. Systems Development Methodology Controls

(1) The system development process should include detailed system analysis and design.

(2) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost and/or benefit analysis, and be used to prepare the computer programs.

11. • Submit SDP to LCM review and milestone approval authority.

a. Policies, Standards, and Procedures

(1) Rigorous AIS budgeting procedures should be implemented to ensure that all significantly ADP-related initiatives, expenditures, and reprogramming are clearly highlighted, whether or not they fall within budget decision units or are spread over multiple decision units.

D. Development (Phase 3)

1. • Mission Need Reaffirmed.

a. AIS Planning

(1) Regular internal audit review and reporting should be conducted regarding completed and proposed planning decisions in relation to mission requirements.

2. • Develop Computer Programs and Data Bases.

a. AIS Planning

(1) The planning process should measure and compare actual accomplishments with expected performance throughout the system life cycle.

b. Systems Development Methodology Controls

(1) The system development process should include programming.

(2) Additional hardware and system software requirements should be consistent with AIS plans and be included in the cost and/or benefit analysis, and be used to prepare the computer programs.

(3) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost-benefit analysis, and be used to prepare the computer programs.

(4) Program and system test results should be reviewed and signed by the system analyst.

(5) Sufficient computer time should be allocated for the conversion process.

(6) The system should be “acceptance tested” by a group independent of the programmers and analysts who designed the system to ensure that it performs in accordance with specifications and meets user needs.

(7) The system acceptance group should certify in writing that the system performs in accordance with all functional and performance specifications.

(8) This group should control all changes to the system to maintain its integrity on a continuing basis.

(9) The following personnel should be involved in the system development process: project managers users, system analysts, programmers, acceptance testers, and internal auditors.

(10) The duties of the personnel on the development project should be clearly separated.

(11) Specific tasks and timeframes for completing the tasks should be established for each member of the development project.

(12) The project manager should be authorized to make decisions on personnel resources, scheduling and most technical project matters.

(13) A management project steering committee should be formed to oversee and review progress throughout the life cycle.

(14) Users should actively participate in system development .

c. Program Testing and System Acceptance Controls

(1) Programming and software packages should be used to improve computer programs' efficiency and effectiveness.

3. System Support Documentation Developed (User's Manuals).

a. Malfunction Reporting and Preventive Maintenance Controls

(1) Formal malfunction reporting procedures should be established and documented for the data processing installation.

(2) Computer operators should be required to keep logs of all computer processing actions.

(3) These logs should record start ups, errors, reruns, recoveries, shut downs, shift changes, and maintenance occurrences.

(4] Log pages should be sequentially numbered.

(5) All processes and operator decisions should be recorded chronologically in the operations log.

(6) Console log pages should be sequentially numbered.

(7) Formal preventive maintenance procedures should be established and documented for the data processing organization.

b. Technical Controls

(1) The vendor or developer of the security software should provide a completely documented description of its design and operation.

(2) Security software functions should be adequately supported by proper manual procedures.

(3) Library procedures should be documented.

(4) External labeling procedures should be documented.

c. Disaster Avoidance and Recovery

(1) These control procedures need to be formally documented and periodically tested and updated.

(2) Emergency procedures should be formally documented and distributed to all associated personnel.

(3) Backup arrangements should be documented and formally agreed upon by all parties concerned.

d. Operating Systems Controls

(1) A complete documented description of the operating system' s design and operation should be provided by the vendor or developer.

e. System Utilities Controls

(1) The vendor or developer of the system utilities should provide a complete documented description of their design and operation.

(2) A complete directory of all available utilities should exist.

f. Program Library Systems Controls

(1) A program library system should be used to control application programs.

(2) The program library system should restrict access to application programs, control movement of programs from test to production modes, control movement of programs from source code to object code, and control changes to applicat ion programs.

(3) Control functions performed by the program library system should be protected so they cannot be bypassed.

(4) The vendor or developer of the program library system should provide a complete documented description of the system's design and operation.

(5) program library system functions should be adequately supported by proper manual procedures.

g. File Maintenance Systems Controls

(1) The vendor or developer of the file maintenance system should provide a complete documented description of its design and operation.

(2) File maintenance system functions should be adequately supported by proper manual procedures.

h. Data Communications Systems Controls

(1) The vendor or developer of the data communications system should provide a complete documented description of its design and operation.

(2) Data communications system functions should be adequately supported by proper manual procedures.

i. System Software Change Controls

(1) All relevant documentation should be changed to reflect system software modifications.

(2) System software changes should be thoroughly tested to ensure that modifications function properly.

(3) System software modifications should be subjected to a system acceptance test before being placed in operations.

j. Distributed Processing and Network Operations Controls

(1) Summary control reports should be distributed to all network user organizations.

(2) Written procedures should exist for switching to backup equipment, files, or systems.

(3) Remote users should have a list of standard terminal, modem, and controller device settings to facilitate problem determination.

k. Systems Development Methodology Controls

(1) The system development process should include procedure preparation.

(2) Procedures should exist to ensure that no data is lost or erroneously changed during conversion to the newly designed system.

l. System Reporting Documentation Controls

(1) A plan should be documented to test the system.

(2) A test analysis report should be developed to document the test analysis results and findings.

(3) A users or procedures manual should be developed to document the functions of the system

(4) An operations manual should be developed to describe the system and its operational environment for computer operations personnel.

(5) A program maintenance manual should be developed to give the maintenance programmer sufficient information to understand the programs, their operating environment and their maintenance procedures.

(6) There should be signatures or other documented evidence of who performed systems and programming work.

(7) Ensure that programmers implement established standards for documenting different data processing functions.

m. Data Origination Controls

(1) Documented procedures should exist to explain the methods for source document error detection, correction, and reentry.

n. Data Input Controls

(1) Documented procedures should exist to explain the methods for data conversion and entry.

(2) Documented Procedures should exist to explain the process of identifying, 'correcting, and reprocessing 'data rejected by the application.

o. Data Processing Controls

(1) Documented procedures should exist to explain the methods for proper data processing of each application program.

(2) Operator instructions should include system start-up procedures, backup assignments, emergency procedures, system shutdown procedures , error message debugging instructions, and system and job status reporting instructions.

p. Data Output Controls

(1] Documented procedures should exist to explain the methods for proper balancing and reconciliation of output products .

(2) Documented procedures should exist to explain the methods for proper handling and distribution of output reports.

q. Program Change Controls

(1) User authorization and written approval should be required for all program changes .

(2) AIS project management authorization and written approval should be required for all program changes.

4. " Unit and System Level Test Performed.

a. System Software Change Controls

(1) System software changes should be thoroughly tested to ensure that modifications function properly.

(2) System software modifications should be subjected to a system acceptance test before being placed in operations.

b. Distributed Processing and Network Operations Controls

(1) Users should participate in acceptance test, review test results; and provide approvals for functions over which they have jurisdiction.

c. Systems Development Methodology Controls

(1) The system development process should include testing.

(2) Upon completion of all programming, each program, interrelated subsystem and the entire system should be thoroughly tested.

(3) Program and system test results should be reviewed and signed by the system analyst.

(4) Prior to acceptance testing, the newly designed system should be tested in parallel operations with the old system.

d. System Reporting Documentation Controls

(1) A plan should be documented to test the system.

(2) A test analysis report should be developed to document the test analysis results and findings.

e. Program Testing and System Acceptance Controls

(1) Each program, subsystem, and then the entire system should be tested.

(2) Test data should be treated like live data, as opposed to entering codes in the test data to indicate that it is not normal production data. When using test data in a live system, it would be mandatory to make it as test data.

(3) System acceptance transactions should be tested like live transactions, as opposed to having special codes entered in the transaction to indicate that it is not normal product ion data.

(4) Sufficient volumes of test and system acceptance transactions that have a wide range of valid and invalid conditions should be entered and processed.

(5) Sufficient time should be allocated for thorough testing and system acceptance purposes.

(6) Sufficient staff members should be allocated for testing and system acceptance purposes.

(7) Test cases and system acceptance test transactions should be developed to review:

(a) Mainline and end-of-job logic.

(b) Each routine.

(c) Each exception.

(d) Abnormal end-of-job conditions.

(e) Combinations of parameter cards and switch settings.

(f) Unusual mixtures and sequences of data.

(g) Control features; e.g., salary parameters.

(8) Test and system acceptance data should include cases that test for the following:

(a) Codes.

(b) Characters.

(c) Fields

(d) Combination of fields.

(e) Transactions.

(f) Calculations.

(g) Missing data.

(h) Extraneous data.

(i) Amounts.

(j) Units.

(k) Composition.

(1) Logic decisions.

(m) Limit or reasonable checks.

(n) Sign.

(o) Record matches.

(p) Record mismatches.

(q) Sequence.

(r) Check digit.

(s) Cross footing of quantitative data.

(t) Control totals.

(9) New programs should be run parallel to old ones to help ensure their accuracy.

5. • (Computer Resource Acquisition Strategy Implemented (hardware, software & services acquired) .

0 Product Control Through Conf igurat ion Management Implemented.

a. Systems Development Methodology Controls

(1) The system development process should include operations.

6. • Logistics Support and Training Plans Finalized.

a. Organizational Controls

(1) Training programs should exist to maintain and build skills, knowledge and ability in systems technology, as well as internal control and ADP security requirements .

b. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

c. Distributed Processing and Network Operations Controls

(1) Documentation and training should be provided to all network operations personnel.

7. " Product Acceptance Criteria Finalized. Products Evaluated.

a. Internal Audit

(1) Internal audit should review application controls of computer-based systems to assess their reliability in processing data in a timely, accurate, and complete manner.

(2) These control reviews should ascertain whether the systems conform to both organization and Federal standards.

b. Systems Development Methodology Controls

(1) The system development process should include system acceptance.

(2) Upon completion of all programming, each program, interrelated subsystem, and the entire system should be thoroughly tested.

(3) The system should be "acceptance tested" by a group, independent of the programmers and analysts who designed the system, to ensure that it performs in accordance with specifications and meets user needs.

(4) The system acceptance group should certify in writing that the system performs in accordance with all functional and performance specifications .

c. Program Testing and System Acceptance Controls

(1) All computer programs should be checked by the programmer and his/her supervisor through desks checks or walk throughs before program assembly or compilation.

(2) All computer programs should be reviewed after assembly or compilation to ensure that errors disclosed by these routines are corrected.

(3) System acceptance should be performed using test data similar to, but independent of, program testing data.

(4) All computer-based systems should be subjected to a system-acceptance process.

(5) The system acceptance should evaluate whether the entire system, both manual and automated processes, is performing in accordance with system specifications and processing standards.

(6) System acceptance should be performed by individuals independent of those who performed the analysis, design, and/or development of the system.

(7) Once system acceptance has been completed, a written certification that the entire system performs in accordance with all functional and performance specifications should be required before the system is placed in operation.

8. . Operations and Deployment Plans Finalized.

a. Organizational Controls

(1) The ADP function should be placed sufficiently high in the organization to ensure its independence from other site operations.

(2) Major organizational units within ADP should be described and their" responsibilities delineated and documented.

(3) Where practical, the following functions should be performed by a different individual or group:

(a) Systems analysis.

(b) Application programming.

(c) Acceptance testing.

(d) program change control.

(e) Data control.

(f) Production control and scheduling.

(g) Computer equipment operation.

(h) System software maintenance.

(i) Computer files maintenance.

(j) Source document origination.

(k) Source document conversion to machine-readable format.

(4) Transactions generally should originate and be authorized in an organization outside of ADP.

b. User Billing and Charge-back Controls

(1) Procedures for user billing and charge should be documented.

(2) Billing and charge-back agreements should exist between users and the data processing organization.

(3) The user billing charge-back procedures should be effectively tied into a job accounting system for the data processing resources.

(4) The user billing and charge-back procedures should be based on the number of transactions processed, on an artificial "computer accounting unit", or some other equitable method.

(5) Adequate procedures should exist for determining the share of system development costs plus additional overhead items, such as lighting, space, and air conditioning, for billing users.

(6) Additions and replacements of hardware,, software, should be justified on the basis of resource utilizat ion and user needs.

(7) An equitable procedure should exist for charging reruns of productions jobs so that user errors are charged back to users, while data processing organization errors are absorbed by data processing.

c. Workload Scheduling Controls

(1) The control group should establish and document formal scheduling procedures, schedule product ion runs and other workloads, and reschedule aborted or erroneous processing.

(2) The control group should be responsible for recording and controlling the production data processed by the data processing organization.

d. System Software Change Controls

(1) Formal documented system software change procedures should be established.

(2) Procedures should be established to ensure that emergency system software modifications are immediately subjected to a system acceptance test.

(3) Procedures should be established so that the accepted emergency modifications-will be incorporated into the next operational version of the system software.

e. Distributed Processing and Network Operations Controls

(1) The distributed processing requirements definitions should be responsive to management objectives in

terms of the hardware configuration, data base configuration, and hardware and communications network interface.

(2) Network data policies should require that data set ownership be clearly established.

(3) User and system responsibilities should be fully defined for coordinating and reconciling differences between distributed and/or replicated data bases prior to network implementation.

(4) Reconciliations should be able to be satisfactorily performed under normal conditions, following network failures, and between varying application problems.

(5) Network asset inventories should be maintained at respective facilities and be periodically reviewed against actual network facilities.

(6). Effective hardware and software backup provisions should exist for the entire network and for the individual facility.

(7) Local and consolidated network performance reports should be established to regularly report key elements such as network system availability, performance to schedules, response times, processing facility efficiencies and performance problems.

f. Data Origination Controls

g. Data Input Controls

9. " Economic Analysis Updated

a. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

10. .Preparation of System Decision Paper (SDP III).

11. . Submit SDP to LCM review and milestone approval authority.

a. Policies, Standards, and Procedures

(1) Rigorous ADP budgeting procedures should be implemented to ensure that all significantly AIS-related initiatives, expenditures, and reprogramming are clearly highlighted, whether or not they fall within budget decision units or are spread over multiple decision units.

E. Deployment (Phase 4) and **Operat** ion (Phase 5)

1. " Implement Operational And Deployment Schedule

a. Administrative Controls

(1) Risk assessment studies should be performed at least every 5 years.

(2] The mission analysis process should be considered an on-going, continuous process **through** the life cycle, to ensure that both present and future data processing **needs** are satisfied.

(3) Requirements should be established for conducting risk analysis for DoD Government-owned, **contractor-** operated facilities and for Government-operated facilities.

(4) Responsibility should be assigned for computer security at each ADP facility.

(5) Individuals assigned responsibility for computer security should be given training and experience in both the computer and security areas.

(6) Plans should provide for assessing risks related to computer services provided by other agencies and those provided through commercial services.

(7) Employees utilizing ADP equipment and processing DoD data should be required to sign an agreement regarding their role and responsibility at the facility and in the ownership and use of data processing equipment and information within the data center.

(8) Personnel security policies for screening employees and contractor and/or service personnel should be established and provide for levels of screening commensurate with the sensitivity of the position or function.

(9) Procedures should exist to handle a situation in which an employee becomes a suspected security risk.

b. Physical Controls

(1) Written procedures should exist to define **restrictions** to computer room access.

(2) A reliable guard service or alarm system should exist to protect the computer center against illegal entry, vandalism, or sabotage.

(3) Access to the computer areas should be restricted to only authorized and appropriate personnel through

the use of a passcard system, combination locks, security badges, or other appropriately secure means.

(4) Combinations on locks or similar devices should periodically be changed.

(5) Account codes, authorization 'codes, passwords, should be controlled to prevent unauthorized use.

(6) Restricted entrances and emergency exits should be equipped with tamperproof automatic alarm systems that signal when doors are opened.

(7) Exterior walls, tape library walls, storage room walls, should be of solid construction from floor to ceiling.

(8) Data processing personnel should be trained to challenge improperly identified visitors.

(9) Data Processing Personnel should be counseled to report all intentional or inadvertent cases of security intrusions of which they become aware.

(10) Access to the computer area by custodial, electrical and other in-house maintenance personnel should be supervised and controlled.

(11) Vendor and support personnel should provide positive identification before they can be admitted to the computer area.

(12) At least two individuals should be present in the computer room at all times.

(13) A procedure should exist to restrict access to source documents. and blank input forms to authorized employees.

(14) All critical forms, such as identification cards, negotiable instruments, and source documents, should be prenumbered for accountability, stored in a secure location, and periodically accounted for.

(15) Procedures should exist to limit access to critical forms during their intermediate storage and transportation, such as dual custody and mail message carrier controls.

(16) A procedure should exist for joint authorization of releases from the storage areas, and the receipt of critical forms should be inventoried by two people at the time of delivery.

(17) procedures should be established to control the issuance of critical forms for jobs scheduled for processing.

(18) Copies of critical outputs that need to be destroyed should be kept in a secure location until they can be destroyed.

(19) At least two people should be present when critical outputs are destroyed.

(20) Periodic billing statements should be provided to user departments describing cost details and the billing algorithm used.

c. Disaster Avoidance and Recovery

(1) The computer center should be separated from adjacent areas by fire resistant partitions and/or walls, and non combustible materials should be used in the center.

(2) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center.

(3) Heat and smoke detectors should be installed in the ceiling, under raised floors, and in the air ducts, alerting the local fire department as well as internal personnel.

(4) Portable fire extinguishers should be located in strategic and accessible areas, be vividly marked, and be periodically tested.

(5) Emergency exits and evacuation routes should be clearly labeled, and battery-powered emergency lights should be placed in strategic locations to assist in evacuation should the power be interrupted.

(6) The computer center should be protected by an automatic fire suppression system.

(7) Emergency switches for cutting off power should be easily accessible near the data center exits.

(8) Emergency power shutdown should include the air conditioning system.

(9) Either the computer center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and humidity in the computer center and take appropriate actions as necessary.

(10) The computer center should be air conditioned by a separate system sufficiently protected from unauthorized access and made from noncombustible materials.

(11) Air intakes should be protected against the introduction of noxious substances.

(12) Backup air conditioning should be available.

(13) The source of electric power should be sufficiently reliable to ensure continued operations and be adequately protected from unauthorized access.

(14) The computer center should be backed up by an uninterruptible power source system.

(15) At least one file generation should be kept at a location other than the file storage area.

(16) Copies of critical files, application programs, system software programs and critical documentation should be stored at an off-site location and be restricted from unauthorized access.

(17) Backup computer capacity should exist within the computer center and at an off-site location.

(18) Critical locations should be provided with the backup devices of terminals, modems, and communication lines.

d. Technical Controls

(1) A list of all personnel should exist and be periodically reviewed by supervisors detailing what computer resources the personnel have access to.

(2) The responsibility for issuing and storing disk packs, magnetic tapes, or other data storage media should be assigned to a librarian. This responsibility should be the librarian's chief function.

(3) Library procedures should be documented.

(4) Access to the library should be limited to authorized personnel.

(5) A librarian should be on duty whenever the data center is being used.

(6) Sensitive files, such as security classifications or Privacy Act restrictions (reference (l)), should be properly identified as such, and appropriately secured.

(7) To prevent release to unauthorized personnel, all data files should be logged in and out.

(8) All files should be expeditiously returned to the library after use.

(9) Disk packs and tape inventory records should be kept.

(10) External labeling procedures should be documented.

(11) External labels should be affixed to active disks and/or tapes.

(12) Work or scratch tapes should be kept in separate areas of the library.

e. AIS Planning

(1) Regular internal audit review and reporting should be conducted regarding completed and proposed planning decisions in relation to mission requirements.

f. Policies, Standards, and Procedures

(1) All appropriate organizational components of the site involved with ADP systems should be defined and clearly assigned their respective areas of functional responsibility.

g. Distributed Processing and Network Operations Controls

(1) Documentation and training should be provided to all network operations personnel.

(2) Network asset inventories should be maintained at respective facilities and be periodically reviewed against actual network facilities.

(3) Effective hardware and software backup provisions should exist for the entire network and for the individual facility.

(4) Procedures stating the preferred method for disposing of sensitive network documents at remote locations should exist and be communicated to the appropriate personnel.

(5) Network availability and reporting, timing and/or response, storage, backup, and functional control requirements for all applications should be established by users and communicated to the responsible network operations organization.

(6) All network facilities should communicate with each other on a regular basis to discuss schedules and coordinate processing requirements and operating procedures.

(7) All network facilities should prepare schedules of consumable needs so that resources can be efficiently and effectively distributed throughout the network.

(8) Remote and local network control terminals, and operations personnel authorized to use them, should be identified.

(9) All outgoing messages and/or data units should be edited for valid destination addresses.

(10) When encryption is in use, the individual assigned the responsibility of management should not be involved with the operation or processing of data.

(11) Remote users should have a list of standard terminal, modem, and controller device settings to facilitate problem determination.

(12) Local and consolidated network performance reports should be established to regularly report key elements, such as network system availability; performance to schedules, response times, processing facility efficiencies and performance problems.

(13) External labels should be used on cables, modems , control units, and other hardware devices to expedite fault isolation and service.

(14) Communications provisions should exist to temporarily store messages and/or data units destined for remote facilities not in service and for reactivating them when service is resumed.

(15) Procedures should exist at remote facilities to ensure that all changes made to operating systems software are effectively controlled and made immediately visible to the control group directly responsible for the overall network.

(16) Local and/or private communications lines and switches should be adequately secured and accessible only by authorized personnel.

(17) Consolidated security reports should be periodically published reflecting recent network security reviews, and they should be available to all network user organizations.

(18) Adequate security measure should be in force at the backup facility.

h. Data Origination Controls

(1) This control group should verify that source documents are complete and accurate. Furthermore, all documents should be accounted for, be transmitted in a timely manner and have been appropriately authorized.

(2) A separate user group should perform the input function when the user organization is responsible for its own data entry.

(3) The control group should identify errors to facilitate the timely correction of erroneous information.

(4) Error logs should be used to ensure" timely follow-up and correction of unresolved errors.

(5) Originators of source documents should be notified by the control group of all errors.

(6) Blank source documents should be stored in a secure locat ion.

(7) When transmitted for conversion, source documents should be transported in accordance with their security classifications.

(8) Source documents should be retained as a safeguard against data loss or destruction during subsequent processing.

(9) Source documents should have specific retention periods.

(10) Source documents should be stored in a logical manner to facilitate retrieval.

(11) Whenever a source document leaves the originating organization, a copy should be kept in the organization.

(12) When reaching their expiration dates, source documents should be removed from storage and destroyed in accordance with the approved disposal schedule.

i. Data Input Controls

(1) Data entry terminal devices should be locked in a physically secure room.

(2) The work entered on a terminal should be restricted by the authority level assigned to each terminal.

(3) Individual passwords should be changed periodically.

(4) Passwords should be deleted once an individual changes his or her job function or level of access.

(5) Management should review unauthorized usage reports.

(6) Management should periodically review the propriety of the terminal authority levels.

(7) Each individual user of the on-line system should be limited to certain types of transactions .

(8) Corrections should be reviewed and approved by supervisors before reentry, if appropriate.

(9) procedures for processing corrected transactions should be the same as those for processing original transactions, except for the supervisory review and approval.

(10) The ultimate responsibility for the completeness and accuracy of all application processing should remain with the user.

(11) The terminal user should correct errors caused by data conversion or entry.

(12) The user originating the transaction should correct errors not caused by data conversion or entry.

(13) Debit and/or credit entries, rather than delete or erase commands, should be used to correct errors on the suspense file.

(14) All documents entered into the application should be signed or marked in some way to prevent accidental duplication or reuse of the data.

(15) The data processing organization should have a schedule by application showing when data requiring conversion and when data requiring entry wi 11 be received and needs to be completed.

(16) The data processing organization should have a control group responsible for data conversion and entry of all source documents received from users .

(17) This group should account for all batches of source documents received from the user to ensure that no batches have been added or lost .

(18) This group should independently develop record counts and predetermined control totals to be balanced with those of the control group in the user organization, and all discrepancies should be reconciled.

j. Data Processing Controls

(1) The data processing organization should have a schedule showing when each application program is to be run and needs to be completed.

(2) The data processing organization should have a control group responsible for controlling all data processing operations.

(3) The log should routinely be reviewed by supervisors to determine the cause of problems and the appropriateness of actions taken.

k. Data Output Controls

(1) The data processing organization should have a control group that is responsible for reviewing all outputs produced by the application.

(2) This group should monitor the processing flow to ensure that programs are processed according to schedule.

(3) This group should review output products for general acceptability and completeness.

(4) This group should reconcile each output batch total, record count an-d predetermined control total with input batch totals, record counts and predetermined control totals before releasing any reports to ensure that no data was added or lost during processing.

(5) These logs should be reviewed by supervisors to determine the correctness of output production.

(6) A transaction log kept by the application should be compared regularly with a transmission log kept at each output device to ensure that all transactions have been properly processed to the final output steps.

(7) The user should have a control group that is responsible for reviewing all output received from the data processing organization.

(8) This group should be given lists of all changes to the application master file data and programmed data, of all internally generated transactions produced by the application, of all interface transactions processed by the application, and of all transactions entered into the application.

(9) This group should use these lists to verify the accuracy and completeness of all output.

(10) This group should verify all computer-generated batch totals, record counts and predetermined control totals with its own manually developed batch totals, and record counts and predetermined control totals.

(11) The user should retain ultimate responsibility for the accuracy of all outputs.

(12) A priority system should exist to ensure that critical outputs are produced on t ime.

2. " Formal Change Control Process.

a. System Software Change Controls

(1) Formal documented system software change procedures should be established.

(2) Change request forms or other documentation should be used to originate system software modificat ions , with all forms sequentially numbered and accounted for.

(3) Access to data files and application programs should be denied to the system programmer making a system software modification.

(4) The system programmer making an emergency modification should be denied access to data files and application programs that were operating when the problem occurred.

(5) The system programmer making "an emergency system software modification should complete a signed statement and leave it with the computer operator as to the encountered problem and its solution.

b. Systems Development Methodology Controls

(1) This group should control all changes to the system to maintain its integrity on a continuing basis.

(2) System implementation should be coordinated with all personnel involved and other systems affected.

c. Program Change Controls

(1) Formally approved written standards for program changes and documentation should exist and be followed.

[2) Procedures defining who can initiate and who can authorize change requests should be established.

(3) Change requests should be written, including a description of the nature of and reasons for the proposed change as well as security and privacy specifications.

(4) Change requests should be made by users on sequent i ally numbered forms.

(5) User authorization and written' approval should be required for all program changes.

(6) AIS project management authorization and written approval should be required for all program changes.

(7) Changes should be approved by individuals who do not operate the computer, except for microcomputers.

(8) Procedures should exist to ensure that all program changes, both scheduled and emergency, are subjected to the testing and acceptance process.

(9) Application changes should be tested prior to operational use.

(10) Modified programs should be tested under normal operating conditions.

(11) Users should be involved in preparing test data and reviewing test results.

(12) Test results should be reviewed with supervisory personnel before revisions become effective.

(13) All errors detected during the conversion process should be investigated before and after correction.

(14) Cert ificat ion should be made that test results demonstrate adequate protection from fraud, waste, and misuse of the program.

(15) All program changes should be documented, and appropriate program, 'sys-tem, oper-at ions , and user documen-tat ion should be updated as changes are made.

(16) A log should be maintained of all completed changes and all changes in progress.

(17) Program changes should be documented by individuals who do not operate the computer.

(18) Certification should be made that documentation specifications are met .

(19) Program library software should be used to report all changes to ADP managers and to users.

(20) Assurances should be made that changes meet users' needs.

(21) Procedures-should exist to determine if any other system is affected by the program modification.

(22) Original programs should be retained until changes have-been processed and new programs tested and updated.

(23) Once modifications have been implemented, procedures should prevent original programs from being used by mistake.

(24) Procedures should be in place to ensure that an "abnormal" volume of regularly scheduled program modifications results in a review to determine if a problem exists with programs, procedures, or the computer-based system.

(25) A limit should be placed on the frequency of program changes, except for emergency changes.

(26) When emergency changes are made, both the user and ADP project manager should be notified.

(27) All problems related to program changes should be documented and given to the ADP project manager.

3. . Periodic Reviews and Audits.

a. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

(2) The planning process should measure and compare actual accomplishments with expected performance throughout the system life cycle.

b. Internal Audit

(1) The internal auditors charter should allow the conduct of independent reviews and the reporting of findings and recommendations to the site's management.

(2) Periodic audits should be designed to test both internal controls and reliability of processed data.

(3) When appropriate, internal audit should verify the information on output reports against related source documents.

c. Workload Scheduling Controls

(1) A formal control group should be established within the data center to monitor both remote decentralized as well as centralized job entry.

(2) Formal input and/or output control procedures should be established and documented.

(3) All totals should be balanced during and after applications processing, and all processing errors should be controlled by the control group.

(4) An authorization document or a transmittal sheet should be required to accompany all input transactions.

(5) All output reports should be visually scanned by the control group for general accuracy and completeness and be distributed according to a formal schedule.

(6) A priority scheme of classes or priorities should be used for scheduling work.

(7) Source documents should be maintained for reference in a logical sequence until the scheduled time of disposal.

(8) The mix of on-line and batch jobs should be scheduled to promote efficient use of facilities and to meet user requirements.

(9) A systematic time-related flow of jobs through each work center should be established.

(10) Rush or rerun jobs should be scheduled consistent with their priority ratings.

(11) Approximate elapsed time of delay should be recorded for each delay event .

(12) In on-line systems, response time statistics should be kept and monitored for significant fluctuations in response time.

(13) CPU utilization statistics should be monitored for both batch and on-line processing.

(14) Significant variances in performance should be followed up by the control group.

d. Malfunction Reporting and Preventive Maintenance Controls

(1) The computer system should automatically produce a log of **all** system operations.

(2) Disposition notes should be entered on the console log showing corrective actions taken when unscheduled program halts occur.

(3) Job reruns should be recorded along with their reason on the console log.

(4) Logs should be reviewed and signed at the end of each shift by a supervisor and filed according to the authorized retirement schedule.

(5) Logs should be independently examined to detect operator problem and unauthorized **intervent** ion.

(6) System crashes should be isolated and identified by cause..

(7) System performance records should be maintained.

(8) Logs of the type and time of maintenance performed **should** be kept.

(9) A schedule for machine maintenance should be published and followed.

(10) The production schedule should be flexible enough to accommodate preventive maintenance.

(11) Preventive maintenance should not be scheduled during peak load periods.

(12) Rush or rerun jobs should be scheduled consistent with their priority ratings.

(13) Approximate elapsed time of delay should be recorded for each delay event.

(14) In on-line systems, response time statistics should be kept and monitored for significant **fluctuat** ions in response time.

(15) CPU utilization statistics should be monitored for both batch and on-line processing.

e. User Billing and Charge-back Controls

(1) Billing and charge-back agreements should exist between users and the data processing organization.

(2) The user billing charge-back procedures should be effectively tied into a job accounting system for the data , processing resources.

(3) The user billing and charge-back procedures should be based on the number of transactions processed, on an artificial "computer accounting unit ," or some other equitable method.

(4) Adequate procedures should exist for determining the share of system development costs plus additional overhead items, such as lighting, space, and air conditioning, for billing users.

(5) Additions and replacements of hardware, software, should be justified on the basis of resource utilization and user needs.

(6) Periodic billing statements should be provided to user departments describing cost details and the billing algorithm used.

f. Disaster Avoidance and Recovery

(1) These control procedures need to be formally documented and periodically tested and updated.

g. Distributed Processing and Network Operations Controls

(1) All network locations should receive regularly scheduled hardware preventive maintenance and log all hardware problems.

(2) A comprehensive post-implementation technical review of the network should be required and performed by systems personnel.

h. Systems Development Methodology Controls

(1) The system development process should include post-implementation audit .

(2) A post-implementation audit of the entire system, manual and automated, should be performed by the internal audit staff after the system has been in operation for several months .

i. Data Input Controls

(1) The suspense file should periodically be analyzed to determine whether too many errors are being made and whether corrections are being processed in a timely manner.

(2) The data processing organization should have a schedule by application showing when data requiring conversion and when data requiring entry will be received and needs to be completed.

(3) The control group should account for all batches of source documents received from the user to ensure that no batches have been added or lost.

(4) This group should independently develop record counts and predetermined control totals to be balanced with those of the control group in the user organization, and all discrepancies should be reconciled.

j. Data Output Controls

(1) Users should periodically be questioned to determine whether they find the reports they receive relevant; whether they find the data presented on reports accurate, reliable and useful; whether they should be removed from or added to distribution lists for receiving reports; and whether they have suggestions concerning the format, content, frequency, and timeliness of reports they receive.

k. System Utilities Controls

[1) Computer operators should be denied access to system utility documentation.

1. Program Library Systems Controls

(1) Computer operators should be denied access to all libraries maintained by the program library system.

4. . Maintain AIS Supporting Documentation

a. File Maintenance Systems Controls

b. Disaster Avoidance and Recovery

(1) Backup procedures should be periodically tested.

(2) Data center personnel should be trained periodically in fire-fighting techniques and be assigned individual responsibilities in case of fire.

(3) Either the computer center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and humidity in the computer center and take appropriate actions as necessary.

(4) A priority scheme should be established at the site and be approved by management, in the event that backup arrangements must be used.

(5) Computer operators should be denied access to all libraries maintained by the program library system.

c. Distributed Processing and Network Operations Controls

(1) Written procedures should exist for switching to backup equipment, files or systems.

d. System Reporting Documentation Controls

(1) Program and system documentation should be accessible to computer operations personnel.

(2) All documentation should be periodically reviewed to ensure that it is current and complete and adheres to established standards.

(3) Copies of all documentation should be stored off the premises.

(4) There should be signatures or other documented evidence of who performed systems and programming work.

(5) Documented procedures should exist for controlling all system documentation.

e. General Environmental Controls

5. " Management and ADP Personnel Concern in Internal Control Techniques.

a. Policies, Standards and Procedures

(1) All appropriate organizational components of the site involved with ADP systems should be defined and clearly assigned their respective areas of functional responsibility.

(2) Customer and/or service interface personnel should be assigned.

(3) ADP resources acquisition, system design, programming, and operating standards should be established, coordinated and communicated to all affected personnel.

b. Organizational Controls

(1) All ADP employees should be prohibited from having authority or duties in any other organization, unless authorized by management.

(2) A direct line of responsibility should exist between every subordinate and supervisor.

(3) A personnel rotation plan should be in effect within the different functional areas in the ADP organization.

(4) ADP personnel should be encouraged to take regularly scheduled vacat ions.

(5) Absentee and turnover rates in the ADP organization should be monitored for potential personnel problems.

(6) ADP position descriptions should be in writing, be clear in delineating authority and responsibility, be kept current, be accompanied by definitions of technical skills needed, and be usable as a basis for performance evaluation.

(7) Personnel recruiting and promotion practices should be based on objective criteria and should consider education, experience, and security risks relevant to the job requirements and to the degree of responsibility.

(8) Before being hired, ADP personnel should be subjected to preemployment checks.

(9) When hired, employees should be provided with an orientation of internal controls and security and with ongoing training to maintain their technical knowledge , skills , and abilities.

(10) Employee performance should be evaluated on a regular basis, and any negative performance should be appropriately addressed.

(11) Policies should be established allowing only authorized personnel use of microcomputer resources to protect the data, software, and physical equipment from improper use or theft.

(12) Proprietary software packages should be protected against copying or modification.

(13) A formal document should state that copyright laws will be rigidly enforced.

(14) Codes, passwords , or other devices should be used to identify authorized users of the microcomputers.

(15) When they are away from the microcomputer area, users of sensitive data should securely lock up all diskettes.

(16) Rooms in which microcomputers are located should be locked after normal working hours.

(17) Microcomputers should be stored in a controlled area.

(18) Property management procedures concerning microcomputer components should be followed, including ma-rking them with unique identification numbers, and recording and securely storing all identification numbers, serial numbers, and equipment descriptions.

c. Workload Scheduling Controls

(1) All personnel should have a copy of a manual detailing required control procedures.

(2) Users should be involved with workload scheduling, except in emergencies.

(3) Operators should not be involved with workload scheduling, except in emergencies.

(4) Reasons for schedule delays should be identified by area of responsibility.

(5) Significant variances in performance should be followed up by the control group.

d. Malfunction Reporting and Preventive Maintenance Controls

(1) Operators and all other appropriate personnel should have access to a manual detailing these control procedures and certify in writing that they have reviewed and understood them.

e. User Billing and Charge-back Controls

(1) Billing and charge-back agreements should exist between users and the data processing organization.

(2) Additions and replacements of hardware, software, should be justified on the basis of resource utilization and user needs.

(3) Rates charged to users should encourage the use of data center resources in accordance with users' needs; differential rates for off-peak usage or the assignment of processing priorities for varying turnaround requirements should

be used to encourage maximum usage of centralized computer facilities.

f. Administrative Controls

(1) Responsibility for conducting risk analyses should be formally assigned,

(2) Responsibility should be assigned for computer security at each ADP facility.

(3) Individuals assigned responsibility for computer security should be given training and experience in both the computer and security areas.

(4) Employees utilizing ADP equipment and processing DoD data should be required to sign an agreement regarding their role and responsibility at the facility and in the ownership and use of data processing equipment and information within the data center.

(5) Personnel security policies for screening employees and contractor and/or service personnel should be established and provide for levels of screening commensurate with the sensitivity of the position or function.

(6) When an employee is terminated, the employee should immediately be denied access to the data processing organization, any data, program listings, and all other employees should be informed of the employee' s terminat ion.

g. Disaster Avoidance and Recovery

(1) Emergency procedures should be formally documented and distributed to all associated personnel.

(2) Procedures should include steps to be taken in the event of an actual or likely natural disaster by fire, water damage, and intent ional damage by sabotage, mob act ion, bomb threats.

(3) The computer center should be separated from adjacent areas by fire resistant partitions and/or walls, and noncombustible materials should be used in the center.

(4) Smoking should be prohibited in the data center.

[5) Data center personnel should be trained periodically in fire-fighting techniques and be assigned individual responsibilities in case of fire. .

(6) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center.

(7) Heat and smoke detectors **should** be installed in the ceiling, under raised floors, and in the air ducts, alerting the local fire department as well as internal personnel.

(8) Portable fire extinguishers should be located in strategic and accessible area, be vividly marked, and be periodically tested.

(9) Emergency exits and evacuation routes should be clearly labeled, and battery-powered emergency lights should be placed in strategic locations to assist in evacuation should the power be interrupted.

(10) The computer center should be protected by an automatic fire suppression system.

(11) Emergency switches for cutting off power should be easily accessible near the data center exits.

(12) Emergency power shutdown should include the air conditioning system.

(13) Either the computer center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and humidity in the computer center and take appropriate actions as necessary.

(14) The computer center should be air conditioned by a separate **system** sufficiently protected from unauthorized access and made" from noncombustible materials;

(15) Air intakes should be protected against the **introduct ion of** noxious substances.

(16) Backup air conditioning should be available.

(17) The source of electric power should be sufficiently reliable to ensure **continued** operations and be adequately protected from unauthorized access.

(14) The computer center should be backed up by an uninterruptible power source system.

(15) Procedures should exist and be applied for the retaining and/or copying of master files as a means of reconstructing a damaged or destroyed file.

(16) Sufficient generations of files should be maintained to facilitate reconstruction of records.

(17) At least one file generation should be kept at a location other than the file storage area.

(18) Copies of critical files, application programs, system software programs, and critical documentation should be stored at an off-site location and be restricted from unauthorized access.

(19) Backup computer capacity should exist within the computer center and at an off-site location.

(20) Critical locations should be provided with the backup devices of terminals, modems, and communication lines.

(21) Backup arrangements should be documented and formally agreed upon by all parties concerned.

(22) A priority scheme should be established at the site and be approved by management in the event that backup arrangements must be used.

(23) Backup procedures should be periodically tested.

(24) Off site materials should be periodically tested.

h. Physical Controls

(1) Data processing personnel should be trained to challenge improperly identified visitors.

(2) Data processing personnel should be counseled to report all intentional or inadvertent cases of security intrusions of which they become aware.

(3) Access to the computer area by custodial, electrical, and other in-house maintenance personnel should be supervised and controlled.

(4) Vendor and support personnel should provide positive identification before they can be admitted to the computer area.

i. Technical Controls

(1) The responsibility for issuing and storing disk packs, magnetic tapes, or other data storage media should be assigned to a librarian.

(2) The responsibility referenced in item 11, above, should be the librarian's chief function.

(3) A librarian should be on duty whenever the data center is being used.

j. System Utilities Controls

(1) Computer operators should be denied access to system utility documentation.

(2) Management authorization should be required prior to the installation and use of new releases of utility programs.

k. Program Library Systems Controls

(1) Obsolete programs should regularly be deleted from the source code and object code library.

1. Data Communications Systems Controls

(1) The authorization code should identify the individual using the terminal and should be periodically changed.

m. System Software Change Controls

(1) Computer operations personnel should have a list of system programmers to notify if the system software requires an emergency or immediate modification.

(2) Access to data files and application programs should be denied to the system programmer making a system software modification.

(3) The system programmer making an emergency modification should be denied access to data files and application programs that were operating when the problem occurred.

(4) The system programmer making an emergency system software modification should complete a signed statement and leave it with the computer operator as to the encountered problem and its solution.

n. Distributed Processing and Network Operations Controls

(1) Effective hardware and software backup provisions should exist for the entire network and for the individual facility.

(2) Adequate disaster and recovery procedures should be developed for each network processing facility. These procedures should be current and.periodically tested.

(2) All network facilities should prepare schedules of consumable needs so that resources can be efficiently and effectively distributed throughout the network.

(4) Records should be maintained on the amount of resources used by each facility.

(S) A comprehensive post-implementation technical review of the network should be required and performed by systems personnel.

(6) A central control function should be established to coordinate control reviews of network assets and resources at all network locations.

(7) Control reviews should be used for assessing the ongoing integrity and overall control of the physical network.

(8) Network output requirements, operating schedules, processing procedures> and facility Coordination policies should be fully established.

(9) policy agreements should exist for communications transmissions including provisions to effectively interface software applications and data bases among coordinated network facilities.

(10) The assignment of transmission priorities should be consistent with established policy and appropriate for the need of the on-line application.

(11) Proper access control should be maintained over the storage and use of network test equipment.

(12) Adequate controls and training regarding distributed data should exist to ensure data compatibility, integrity and effective data usage.

(13) Documentation and training should be provided to all network operations personnel.

i. Systems Development Methodology Controls

(1) The systems acceptance group should control all changes to the system to maintain its integrity on a continuing basis.

6. • Risk Analysis Reassessed.

a. Disaster Avoidance and Recovery

(1) Emergency procedures should be formally documented and distributed to all associated personnel.

(2) The computer center should be separated from adjacent areas by fire resistant partitions and/or walls, and noncombustible materials should be used in the center.

(3) Smoking should be prohibited in the data center.

(4) Data center personnel should be trained periodically in fire-fighting techniques and be assigned individual responsibilities in case of fire.

(5) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center.

(6) Heat and smoke detectors should be installed in the ceiling, under raised floors and in the air ducts, alerting the local fire department as well as internal personnel.

(7) Portable fire extinguishers should be located in strategic and accessible area, be vividly marked, and be periodically tested.

(8) Emergency exits and evacuation routes should be clearly labeled, and battery-powered emergency lights should be placed in strategic locations to assist in evacuation should the power be interrupted.

(9] The data center should be protected by an automatic fire suppression system.

(10) Emergency switches for cutting off power should be easily accessible near the data center exits.

(11) Emergency power shutdown should include the air conditioning system.

(12) Emergency procedures for handling minor and major fires should be-prominently posted throughout the data center.

(13) The computer center should be air conditioned by a separate system sufficiently protected from unauthorized access and made from noncombustible materials.

(14) Either the data center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and

humidity in the computer center and take appropriate actions as necessary.

(15) The data center should be air conditioned by a separate system sufficiently protected from unauthorized access and made from noncombustible materials.

(16) Air intakes should be protected against the introduction of noxious substances.

(17) Backup air conditioning should be available.

(18) The source of electric power should be sufficiently reliable to assure continued operations and be adequately protected from unauthorized access.

(19). The computer center should be backed up by an uninterruptible power source system.

(20) Suff-icient generations of files should be maintained to facilitate reconstruction of records.

(21) At least one file generation should be kept at a location other than the file storage area.

(22) Copies of critical files, application programs, system software programs and critical documentation should be stored at an off-site location and be restricted from unauthorized access.

(23) Backup computer capacity should exist within the data center and at an off-site location.

(24) Critical locations should be provided with the backup devices of terminals, modems, and communication lines.

(25) Backup arrangements should be documented and formally agreed upon by all parties concerned.

o (26) A priority scheme should be established at the site and be approved by management, in the event that backup arrangements must be used.

(27) Backup procedures should be periodically tested.

(28) Off-site materials should be kept up-to-date.

b. Microcomputer Controls

(1) User groups should be required to provide program documentation for approval prior to using application software developed by the group.

(2) A procedures manual should be developed to document the ‘functions and capabi lit ies of microcompute r-based systems.

(3) Approval, requisition, and subsequent placement of microcomputers should be documented.

(4) Management ‘approval and user group concurrence should be secured in instances when data processing personnel modify applicat ion software packages,

(5) Management approval should be secured before application software packages are modified by user groups.

(6) Procedures related to sharing application programs and data should be established.

(7) Management should be established allowing only authorized personnel use of microcomputer resources to protect the data, software, and physical equipment from improper use or theft.

(8) Personnel with appropriate backgrounds should be designated to develop application software and/or to evaluate application software packages offered by vendors.

(9) Acquisition should be justified in terms of objectives and benefits to be realized, and the level of detail in the justification documentation should be kept to a minimum, commensurate with need and judicious management pract ices.

(10) Written guidelines should exist on develop-or-buy alternatives for application software.

(11) Hard disks should be backed up onto another storage medium on a regular basis.

(12) Microcomputers should be stored in a controlled area.

(13) The boot diskette, used to access a hard disk, should be secured.